AMERICAN ALLIANCE FOR VEHICLE OWNERS' RIGHTS
1707 L STREET, N.W., SUITE 560
WASHINGTON, D.C. 20036

March 15, 2021

National Highway Traffic Safety
Administration
U.S. Department of Transportation
1200 New Jersey Avenue, S.E.
West Building Ground Floor
Room W12-140
Washington, D.C. 20590

Re: Comments of the American Alliance for Vehicle Owners' Rights with respect to NHTSA's Updated "Cybersecurity Best Practices for the Safety of Modern Vehicles -- Docket No. NHTSA-2020-0087

Dear Sir or Madam:

The American Alliance for Vehicle Owners' Rights (AAVOR) respectfully submits these comments to the National Highway Traffic Safety Administration (NHTSA) in response to its request for comments on the NHTSA's updated "Cybersecurity Best Practices for the Safety of Modern Vehicles." AAVOR asks that its comments be made part of the official record of this regulatory action.

Description of AAVOR

AAVOR is a diverse group of stakeholders united by the common goal of guaranteeing the right of all vehicle owners to have access to, and control of, the data generated by their vehicles. AAVOR's members represent interests from across the mobility ecosystem, including consumer advocates, fleet owners and operators, shared mobility service providers, automotive repairers, insurers, and telematics providers.

AAVOR's members represent directly and indirectly tens of millions of motor vehicle owners and users – individual vehicle owners and vehicle fleet owners that are key stakeholders in NHTSA's current effort to update its 2016 "Best Practices" document. Unfortunately, the key issues of interest to AAVOR's members – the owners of motor vehicles – are not adequately represented in the draft updated 2021 "Best Practices" document. AVVOR respectfully requests that NHTSA

consider our views, and the issues of importance to vehicle owners, before finalizing the draft 2021 document.

Summary of AVVOR's Concerns with Draft 2021 Best Practices

A fundamental difference of opinion exists between AAVOR's members and motor vehicle manufacturers regarding access to, and control of, data generated by motor vehicles. AAVOR's members stand for the basic proposition that the owner of a motor vehicle must have the ability to access, and to control access to, their own motor vehicle's data. Motor vehicle manufacturers have publicly asserted their right to act as gatekeeper. In this gatekeeper role, the manufacturers further assert an ability to require commercial terms be reached with them for any vehicle owner, or third party, who wishes to have access to the data generated by a vehicle after it is sold. Vehicle manufacturers repeatedly assert "cybersecurity" as the basis for opposing the interest of motor vehicle owners to have direct access to and control of their vehicles' data. AAVOR members have repeatedly demonstrated that both the owner's rights and the need for cybersecurity are able to be protected with technology-neutral and standards-based vehicle architecture. Vehicle manufacturers have significant financial interests in acting as gatekeeper as a means of profit – either through selling telematics or navigation and other services directly to consumers or through commercializing the data harvested from vehicles owned by others.

NHTSA's 2016 Cybersecurity Best Practices document had little or no input from motor vehicle owners or motor vehicle users (or those to which owners provide access to vehicle data such as insurers, telematics companies or automotive repairers), or from the advocates for consumer protection and competition in general. AAVOR has high hopes that NHTSA will adjust its current and future stakeholder consultation practices so that the input of all stakeholders, not just motor vehicle manufacturers and their first-tier suppliers, is sought and incorporated into the final 2021 version of this document and other NHTSA projects that impact consumer safety, consumer protection, and competition.

Key Policy and Technical Issues for Vehicle Owners

AAVOR supports federal and state policies that safeguard individual and commercial fleet owners' rights:

- to access and control their vehicles' data (including authorizing access by third parties such as independent automotive repairers, insurance companies and vehicle manufacturers);
- in a manner that is direct, in-vehicle, intelligible, and in real-time;
- utilizing technology-neutral, standards-based, secure interfaces; and
- that enables interoperable and bi-directional communication with the vehicle.

The rights of vehicle owners to access directly and control the data generated by their vehicles is too important to be left unaddressed by NHTSA in its updated cybersecurity best practices document and by other federal agencies, such as the Federal Trade Commission (FTC) and the

Department of Homeland Security (DHS). In the context of NHTSA's cybersecurity best practice guidance, AAVOR supports NHTSA establishing a framework for securing the continued rights of vehicle owners – and entities that secure the express permission of vehicle owners -- to control vehicle-generated data on a secure and competitive basis.

AAVOR's General Comments on the Draft Updated Cybersecurity Best Practices

To secure these rights, AAVOR urges NHTSA to consider not only the safety aspects of its cybersecurity best practices recommendations but also the impact its recommendations have on consumer protection and competition. NHTSA cannot promote the safety of motor vehicles through cybersecurity best practices in a vacuum. AAVOR posits that NHTSA must consider the interests of motor vehicle owners and federal policies that promote not just vehicle safety but robust consumer protection and vigorous competition among commercial entities. Additionally, AAVOR is ready to bring leading cybersecurity and communications expertise to the conversation, demonstrating clearly that cybersecurity, consumer protection and competition can all be achieved through industry-leading, standards-based solutions.

If NHTSA focuses solely on cybersecurity issues related to vehicle safety in a manner that advertently or inadvertently creates *de facto* monopolies for motor vehicle manufacturers and suppliers over motor vehicle data, then it will sacrifice the equally important federal policy goals of consumer protection and competition. AAVOR urges NHTSA to expand its examination of motor vehicle data cybersecurity issues, perhaps in connection with the FTC (the federal agency responsible for both consumer protection and competition) and the DHS (the federal agency most expert on cybersecurity issues in general).

Specific Examples of AAVOR's Concerns in the Draft Updated Cybersecurity Best Practices

1. Scope of Document -- At the very outset of the draft 2021 update, the section on "Scope" (2.0) confirms that the interests of vehicles owners in the past have not been on NHTSA's "radar screen" in crafting its 2016 Best Practices document. AAVOR respectfully urges NHTSA to add consumers – including motor vehicle owners and users -- to the stakeholders covered by the cybersecurity issues addressed in the draft 2021 update.

2. Cybersecurity Considerations During Vehicle "Use" – In Section 4.2, NHTSA acknowledges that there are cybersecurity considerations during the "use" of motor vehicles by vehicle owners and users. However, throughout much if not all of the rest of the document and its 2016 predecessor, NHTSA focuses on best practices for manufacturers and suppliers to restrict the use of the data being generated by vehicles when driven by their owners or users. AVVOR asks that NHTSA take into account the need of motor vehicle owners to access vehicle data in a cybersecure, direct and real-time manner during the "use" phase of the vehicle's life. Focusing only on the responsibilities and needs of motor vehicle manufacturers and suppliers in the draft 2021 update and prior 2016 document ignores an important set of stakeholders with a keen interest in cybersecurity – consumers, vehicle owners and users

(and entities to which these entities grant data access, such as insurers, automotive repairers and telematics providers).

3. Information Sharing – Section 4.3 -- "As of mid-2020, Auto-ISAC includes 49 organizations." Of those 49 organizations, none of them are consumers, motor vehicle owners or users, either individually or as represented through fleet associations or consumer advocacy groups. AAVOR strongly agrees with NHTSA's recommendation that Auto-ISAC be expanded to include fleet managers and suggests that NHTSA's recommendation be expanded to include individual vehicle owners or users or groups representing individual vehicle owners and users (and third parties to which owners grant data access).

4. Aftermarket/User Owned Devices – Although some vehicle manufacturers embed telematics hardware and software as original equipment, most motor vehicle owners and users secure access to and control of vehicle data through aftermarket devices that are installed by or at the request of the vehicle owner. NHTSA's statement in Section 6 that such user owned devices "could present unique cybersecurity challenges" in AAVOR's opinion reveals an incorrect bias on behalf of the agency in favor of original equipment provided by motor vehicle manufacturers. With respect in particular to cybersecurity concerns, this bias can be misplaced.

   Telematics providers have been awarded contracts to install aftermarket telematics devices in the fleets of the General Services Administration, the Department of Defense, and the Department of Homeland Security (including the Transportation Security Administration and the U.S. Border Patrol). In addition, state and local law enforcement agencies, fire departments and emergency service providers, transportation departments have installed aftermarket telematics devices in their fleets. NHTSA's Section 6 assumption regarding aftermarket devices infers that all of these federal, state and local agencies – including many in the United States' national security network – have installed telematics devices that pose an increased cybersecurity risk. In fact, the opposite likely is true.

5. Limited Access for Aftermarket Devices – Recommended Practice G.40 provides a perfect example of the mistaken assumptions described in paragraph 4 of these comments above. If an aftermarket device possesses the certifications and unauthorized intrusion protections necessary to prevent cybersecurity threats, then there is no reason to limit that device's – and that vehicle's owner's -- access to all of the data generated by a motor vehicle. Again, G.40 contains an inherent assumption that aftermarket devices are less cybersecure than those provided by vehicle manufacturers. AAVOR suggests that NHTSA empirically study the trust of such an assumption prior to embedding it in its final 2021 Best Practices document.

6. Restrictions on Access to Data – Recommended Practice G.43 speaks to motor vehicle manufacturers not "unduly" restrict the ability of third-party repair and maintenance providers from working on motor vehicles. "Unduly" is a very subjective description and open to wide interpretation. What might be "undue" to an independent garage or a motor vehicle

fleet that wants to perform repair and maintenance on its vehicles at its own facility or that of a third party might be defined as reasonable for a motor vehicle manufacturer seeking to force consumers or fleets to have repairs done at branded car dealerships or use only manufacturer replacement parts.

AAVOR suggests that NHTSA reassess the use of the word "unduly" in G.43 due to the subjective nature of the word. NHTSA should, in AAVOR's opinion, be championing cybersecure communications between vehicles and with consumers – such as individual vehicle owners and fleets – not attempted monopolization or anti-competitive practices by motor vehicle manufacturers. At a minimum, with respect to the draft 2021 document, AAVOR request that NHTSA clarify the term "unduly" from G.43.

7. Cryptographic Credentials – AAVOR generally agrees with Technical Best Practices T.3 and T.4, but cautions that NHTSA ensure that these best practices are not interpreted to sanction the encryption of motor vehicle data by manufacturers so as to make it inaccessible to consumers, including motor vehicle owners and users. Again, cybersecurity can be used as a cover for all types of anti-competitive behavior – including encrypting data streams so that consumers and the entities consumers want to have access to this data (telematics providers, repair facilities, insurance companies and others) are preventing from accessing this data due to its encryption.

8. Vehicle Internal Communications – AAVOR disagrees fundamentally with Technical Best Practice T.9, which directs that "critical safety signals should be transported in a manner inaccessible through external vehicle interfaces." T.9 ignores current standard safety, commercial and operational practices in use by motor vehicle owners. Three examples should convince NHTSA that T.9 is misguided and is another example of motor vehicle manufacturers seeking to shut down access to vehicle data and controls for commercial gain and under the cover of cybersecurity concerns.

   For example, many car rental systems, and even some fleets leased by motor vehicle manufacturers, offer "shared mobility" services to consumers. These services permit consumers to "rent"' a vehicle for a short period of time, pick up the vehicle from street parking or a city parking lot that is not a standard car rental facility, and drop the car off after the consumer no longer has need for the vehicle. In a shared mobility service, the functionality of the service is based on the owner of the vehicle being able to unlock the vehicle after the consumer has properly rented the vehicle and is ready to use it. This can only be accomplished through direct, real-time access to the rental vehicle's operational controls through the shared mobility company's wireless connection to its vehicle. Without this access, the entire shared mobility business model fails.

   Second, many trucking companies are able to monitor the performance of the engines of its vehicles through telematic connections. As a truck on its route ascends to higher altitudes, signals can be sent to that truck's electronic control units (ECU) to increase the air/fuel

mixture being fed to the engine to maintain performance and reduce air emissions. Without direct access to such truck ECUs by the trucking company itself, such engine performance adjustments could not be made during the use of the truck.

Finally, many cities and counties are using the telematics signals harvested from their fleet of vehicles (law enforcement, highway maintenance, fire and EMS vehicles, and other government-owned vehicles) to gather information on road conditions, road repair needs, traffic congestion and other information related to important consumer safety and government operations. Again, if direct access to this data is denied to these government agencies due to real or imagined cybersecurity risks, then the consumer and government benefits achieved through these telematics devices will be lost.

9. Wireless Paths into Vehicles – AVVOR agrees in concept with Technical Best Practice T.13 that "all networks and systems external to a vehicle's wireless interfaces" should be authenticated and validated before access to a motor vehicle's systems by such networks and systems is permitted. But to treat such networks and systems as untrusted infers that all networks and systems used by motor vehicle manufacturers are cybersecure and all aftermarket products are not. As noted above, such an inference is misguided and AAVOR suggests that NHTSA not perpetuate the inference through this draft 2021 document.

10. Software Updates – Technical Best Practices T.21, T.22, and T.23 encourage motor vehicle manufacturers to employ only state of the art techniques for vehicle software updates and ensure that updates are undertaken by "authorized and appropriately authenticated parties." AAVOR endorses this approach, provided that it is not interpreted by NHTSA or motor vehicle manufacturers to restrict the ability of consumers, motor vehicle owners and motor vehicle owners to perform such updates independent of the manufacturers – provided such updates are cybersecure and the parties performing the updates are appropriately authenticated.

* * *

AAVOR sincerely appreciates the opportunity to provide these comments on the draft 2021 updated "Cybersecurity Best Practices for the Safety of Modern Vehicles" and trust that our comments will be deemed constructive and helpful. Should AAVOR's comments raise questions or additional issues that NHTSA staff would like addressed, please contact Gregory Scott at 202-297-5123 or gscott@aavor.org.

AAVOR SIGNATORIES TO THESE COMMENTS:

American Bus Association

American Car Rental Association

American Property Casualty Insurance Association

Automotive Recyclers Association

Automotive Service Association

Consumer Action

NAFA – Fleet Management Association

National Consumers League

Owner-Operator Independent Drivers Association

Avis Budget Group

eDriving, LLC

Enterprise Holdings, Inc.

GPS Insight

Geotab, Inc.

Hertz Corporation

Lytx, Inc.

Mix Telematics

Recall Masters

Safelite Group, Inc.

UPS